SEC105

Insider Threat Awareness

SAND2015-9639 TR

This is the PDF version of an online course. It is intended for use with MOWs who do not have SRN access. This file is located in FileNet at:

https://eims.sandia.gov/Workplace/getContent?vsId=%7B7964559F-E170-4F7C-84A8-70428AC050E2%7D&objectStoreName=EIMS._.Content&objectType=document

How to Get Credit 1

Introduction 1

Opening 1

The Insider Threat 1

What Does an Insider Look Like? 2

WikiLeaks 2

Fort Hood Shooting 2

Economic Espionage 3

Indicators of a Potential Insider Threat 3

See What? 3

Major Categories 4

Recruitment 4

Recruitment Indicators 4

Information Collection 5

Information Collection Indicators 5

Information Transmittal 6

Information Transmittal Indicators 6

General Suspicious Behavior 7

General Suspicious Behaviors 7

Reporting 8

Say What? 8

Reporting Procedures 9

Reporting Requirements for DoD 9

Reporting Requirements for Federal Agency Employees 9

Reporting Requirements for Cleared Industry 9

Failure to Report 10

Conclusion 10

SEC105 Certify Completion 12

Feedback Form 12

How to Get Credit

To receive credit for SEC105:

- Read through the course material.
- Follow the directions in the Certify Completion section at the end of this document.

Introduction

Opening

Witness testimony: *I always knew that guy was off. He complained a lot. His schedule was odd. He came in at odd hours. And he asked a lot of questions, maybe too many questions.*

Would you recognize a threat from the inside?

Witness testimony: *But there wasn't really that one thing and it wasn't my place to say anything. It's like a code. We're a team. You don't rat out your team.*

What would you do?

Witness testimony: *I never thought anything like this could happen here.*

If you SEE something, SAY something.

The Insider Threat

Who could become an insider threat? You've probably heard of the notorious cases: those who took secrets and those who took lives; those who risked their organizations and those who risked national security. But there are also unwitting insiders -- people with access to information who unknowingly reveal more than they should.

An insider threat is anyone with authorized access to the information or things an organization values most, and who uses that access -- either wittingly or unwittingly -- to inflict harm to the organization or national security. When an insider becomes a threat, it can have far-reaching consequences on both an organization and national security.

As a cleared employee working for the DoD, a Federal agency, or in cleared industry, you play an important role in protecting against insider threats.

What Does an Insider Look Like?

> Witness testimony: I *was looking for a bad guy. I never thought it could be my friend. I never thought he'd hurt our organization.*

What do insider threats look like? They look like you and me. They look like your friends and neighbors. They can be anyone and they can target anything. Sometimes they are unwitting and simply create vulnerabilities for others to exploit. In addition to classified information, proprietary information, trade secrets, intellectual property, and the security of personnel may be threatened.

Malicious insiders go after anything they can use to inflict harm. They have many motivations: Some do it for money, while others do it for ego. Others do it for a cause or another country. Others do it simply because they can.

There are many cases of insiders betraying the trust of their organizations and their country, including those listed here.

WikiLeaks

The WikiLeaks case represents one of the major catalysts for an insider threat national policy.

In May 2010, an Army Private was arrested for allegedly leaking classified material to the website WikiLeaks. The unauthorized disclosure represents the single largest loss of classified information in U.S. history and includes 250,000 diplomatic cables and 500,000 U.S. Army reports.

Despite reservations stemming from signs of instability, the Private was deployed to Iraq, where he served as an intelligence analyst. As an intelligence analyst, he had access to the DoD's classified networks, SIPRNet and JWICS. During his time in Iraq, he was reprimanded for being persistently late, which led to him overturning a table before being restrained. Shortly after this incident, the Private allegedly began downloading sensitive material, subsequently passing it on to WikiLeaks.

Fort Hood Shooting

In November 2009, an Army Major killed 13 people and wounded 29 others at Fort Hood, Texas. The shooting represents the worst shooting to ever take place at an American military base.

Six months prior to the shooting, the Major had been investigated for expressing extremist views, but was determined not to be a threat as the incident was related to his professional research.

Even before that, when he worked at Walter Reed Medical Center, he had concerned colleagues with his tendency towards conflict and comments concerning the American military presence in Iraq and Afghanistan.

Economic Espionage

Greg Chung, an engineer for a cleared defense contractor, stole over 250,000 documents containing trade secrets about the space shuttle, the Delta IV rocket, and the C-17 military cargo jet. He traveled to China under the guise of giving lectures while secretly meeting with Chinese agents.

In February 2010, he became the first person to be tried under the economic espionage provision of the Economic Espionage Act and was sentenced to over 15 years in prison.

Indicators of a Potential Insider Threat

See What?

Witness testimony: *I always knew that guy was off. But there wasn't really that one thing.*

If faced with a threat from an insider, would you recognize it?

In your day-to-day interactions with your coworkers, you notice the following. Which, if any, may be an indicator of an insider threat?

Select all that apply; then check your answers on the following page.

☐☐ While helping a coworker with a new system, you notice her computer contains Confidential files related to a project she is not working on and has no need-to-know.

☐☐ On your way to a meeting, you overhear two coworkers discussing classified information in an office corridor.

☐☐ During a meeting, a coworker shows off an expensive new watch. When asked about affording such a luxury, he becomes uncomfortable and offers no explanation.

☐☐ As you arrive at your building early one morning, you encounter a coworker leaving the building. The coworker nervously explains that he sometimes prefers to work overnight without the distraction of others.

Major Categories

All of these things might point towards a possible insider threat. Examining past cases reveals that insider threats commonly engage in certain behaviors. For example, most insiders do not act alone.

While some insiders volunteer, others are targeted and recruited by adversary groups. For this reason, you should be aware of common signs someone is being recruited. And once an insider turns on his or her organization, that person will start collecting information. So you need to be able to detect clues that that might be happening. Once they have information, insiders must then transmit it. If you know the signs of information transmittal, you will be better prepared to detect it. And insiders often exhibit other common suspicious behaviors you need to know about.

Not all of these indicators will be evident in every insider threat and not everyone who exhibits these behaviors is doing something wrong. However, most of the insider threats we have discovered displayed at least some of these indicators. It is important for you to be aware of these behaviors so you can combat the insider threat and protect your organization and the country. Let's take a closer look.

Recruitment

> Witness testimony: I *did wonder how he kept up with his bills, but it wasn't my place to say anything.*

While not all insiders are recruited, those who are often recruited slowly over time. Recruitment almost always involves contacts with individuals or organizations from foreign countries. However, an already committed U.S. spy may attempt to recruit colleagues.

Indicators of recruitment include signs of sudden or unexplained wealth and unreported foreign travel.

Recruitment Indicators

Reportable indicators of recruitment include, but are not limited to:

- Unreported request for critical assets outside official channels
- Unreported or frequent foreign travel
- Suspicious foreign contacts
- Contact with an individual who is known to be, or is suspected of being, associated with foreign intelligence, security, or terrorism
- Unreported offer of financial assistance, gifts, or favors by a foreign national or stranger: Beware of those bearing gifts
- Suspected recruitment by foreign or domestic competitive companies to convince employee to work for another company

Information Collection

Witness testimony: *He asked a lot of questions… maybe too many questions.*

Before someone can steal information, they must first collect the information. It can be intentionally stolen by a malicious insider or a person may have it already – and then inadvertently leak it. Insiders may physically remove files, they may steal or leak information electronically, or they may use elicitation as a technique to subtly extract information about you, your work, and your colleagues. When done well, elicitation can seem like simple small talk.

Regardless of the method used, anytime a person attempts to access or record information without authorization, regardless of intent, it should be of concern.

Information Collection Indicators

Reportable indicators of information collection include, but are not limited to:

- Unauthorized downloads or copying of files, especially for employees who have given notice of termination of employment
- Keeping critical assets at home or any other unauthorized place
- Acquiring access to automated information systems without authorization
- Operating unauthorized cameras, recording devices, computers, or modems in areas where critical assets are stored, discussed, or processed
- Asking you or anyone else to obtain critical assets to which the person does not have authorized access
- Seeking to obtain access to critical assets inconsistent with present duty requirements

Information Transmittal

Witness testimony: *Looking back, there were signs. He'd talk about anything - even classified information - anywhere. he didn't care who was around.*

Insiders must have a way to transmit the information they are compromising. If you notice someone showing signs of transmitting information without authorization or outside of approved channels, you should pay attention. Behaviors you might observe include removing assets or information without authorization, extensive use of systems or equipment, and discussing information in unauthorized areas or by unauthorized means.

If you notice someone failing to follow procedures for safeguarding, handling, and transmitting classified information, it may be a sign of an insider threat.

Information Transmittal Indicators

Reportable indicators of information transmittal include, but are not limited to:

- Removing critical assets from the work area without appropriate authorization
- Extensive use of copy, facsimile, or computer equipment to reproduce or transmit critical asset-related information that may exceed job requirements
- Discussing critical asset-related information in public or on a nonsecure telephone
- Actions/behaviors specific to classified information:
- Using an unauthorized fax or computer to transmit classified information
- Attempting to conceal any work-related foreign travel and any personal foreign travel while having a Top Secret/Sensitive Compartmented Information clearance or being a contractor with a reporting requirement
- Improperly removing the classification markings from documents

General Suspicious Behavior

Witness testimony: *I always knew that guy was off. His schedule was odd. He'd come in after hours when no one else was around.*

Once an insider threat is revealed, coworkers often recall signs that something wasn't right. An insider threat may exhibit a number of suspicious behaviors, including working outside of regular duty hours, repeatedly failing to follow processes and policies which result in security violations, or displaying a general lack of respect for the United States.

Special attention should be paid to disgruntled employees. Disgruntlement is a major motivating factor in insider threat cases.

General Suspicious Behaviors

Reportable indicators of other suspicious behavior include, but are not limited to:

- Attempts to expand access:
  - Attempting to expand access to critical assets by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities
  - Performing repeated or unrequired work outside of normal duty hours, especially unaccompanied
- Questionable behavior:
  - Exhibiting behavior that results in repeated security violations
  - Engaging in illegal activity or asking you to engage in any illegal activity
- Changes in financial circumstances:
  - Displaying unexplained or undue affluence explained by inheritance, luck in gambling, or some successful business venture
  - Displaying sudden reversal of financial situation or sudden repayment of large debts

Reportable indicators of general suspicious behavior, continued

- Attempts to compromise individuals:
  - Attempting to entice personnel with access to critical assets into situations that could place them in a compromising position
  - Attempting to place personnel with access to critical assets under obligation through special treatment, favors, gifts, money, or other means
- Questionable national loyalty:
  - Displaying questionable loyalty to U.S. government or company
  - Making anti-U.S. comments
- Exhibits actions or behaviors associated with disgruntled employees:
  - Conflicts with supervisors and coworkers
  - Decline in work performance
  - Tardiness
  - Unexplained absenteeism

Reporting

Say What?

Witness testimony: *We all went to the training. We sat through the briefings. Yet, when we actually saw signs something wasn't right, we did nothing. Why didn't someone say something?*

If faced with a threat from an insider, would you know what to do? Would you know how to report it?

You notice a coworker is demonstrating some of the behaviors of an insider threat. Do you know the channels you should use to report it?

Select your response; then check your answer on the following page.

- ○ Yes, I know exactly what to do and would report it immediately.
- ○ I'm not sure; I'd have to look it up or check with somebody.
- ○ No; I have no idea what I should do… maybe call the hotline?

Reporting Procedures

Witness testimony: *I did feel like something wasn't right. And I did think I should say something. I just didn't know who to go to.*

If you suspect a possible insider threat, you must report it. You cannot assume someone else will do so. Every one of us is an owner of security - both the security of information and the security of personnel. We are all responsible for its safekeeping.

A major hurdle that deters people from reporting is the idea that they are snitching on a colleague. Yet reporting is a way of ensuring your security, the security of your fellow colleagues, and the resources and capabilities of your organization.

Insider threat reporting procedures vary depending on whether you are an employee of the DoD, a Federal Agency, or you work in cleared industry.

Reporting Requirements for DoD

DoD employees must report potential threats to their organization's security office. Security officers will coordinate with counterintelligence elements, if required.

If you suspect recruitment by a foreign entity, report it directly to your supporting counterintelligence element. If you suspect espionage, report to the FBI or counterintelligence officials.

Reporting Requirements for Federal Agency Employees

Federal agency employees should report to their agency's security office. Specific procedures will vary by agency. Follow your agency-specific reporting procedures.

Reporting Requirements for Cleared Industry

Employees of cleared industry must report potential threats to the Facility Security Officer, or FSO. Depending on the situation, the FSO will then report the possible threat to the facility's DSS Industrial Security Representative, DSS Counterintelligence Specialist, or, if it involves known or suspected espionage, to the FBI.

Failure to Report

Witness testimony: *I never thought anything like this could happen. Why didn't someone say something?*

Unfortunately, insider threats often go unreported until it is too late. In the majority of past cases, relevant information was available, yet went unreported. How different might things have been had someone said something?

When you fail to report, you risk both your physical security and the information security of your organization. Insider threats weaken the U.S. military's battlefield advantage and jeopardize war fighters. They increase our vulnerability to fraud, terrorist activity, and cyber-attacks. If you are a member of cleared industry, an insider may cost your company its business and you your job.

Failing to report also fails the employee who needs help. When you don't report, you lose the opportunity to help your coworker resolve problems before committing espionage or hurting others.

For cleared DoD employees subject to Uniform Code of Military Justice, failing to report a potential insider threat may result in punitive actions. For cleared Federal agency and DoD civilian employees, failing to report may result in disciplinary action up to and including termination and criminal and civil sanctions. For cleared defense contractors, failing to report may result in loss of employment and security clearance. Individuals may also be subject to criminal charges.

You cannot underestimate the role you play in protecting against insider threats. You are the first line of defense.

Conclusion

You have just learned how insider threats affect the DoD, Federal agencies, cleared industry, and people like you. You need to be aware of these threats. You need to consider your facility, its technology and programs, and the information you know. How might you be targeted?

If you suspect a potential insider threat, you must report it.

Resources

For those who don't have access to the SRN, email ci-help@sandia.gov or call the CI "hotline" at 505-284-3878 for advice.

Additional resources located on the SRN:

- Security Connection Dial 321 from any SNL phone or 505-845-1321
  (get live assistance to address any security issue and report incidents)

SEC105 Completion Record

- Read through the course material.

- Send your SEC105 Completion Record to Jennifer Roth for credit by any of the following:

E-mail: jroth@sandia.gov
Mail: P.O. Box 5800, Albuquerque, NM 87185-0653
Fax: 505-844-2748

I have read all the modules in Insider Threat Awareness (SEC105).

SNL ID	
Full Name (Print)	
Org.	
Phone Number	
DATE	

Feedback Form

Customer feedback is important to us. Please complete the evaluation form below and forward to Jennifer Roth, MS0653, or fax it to her at (505) 844---2748.

Rate on a scale of 1--- 5 (with 1= poor and 5 =excellent):

The ease of using of this learning tool and/or test?	1	2	3	4	5
The organization of information presented?	1	2	3	4	5
The amount of information presented?	1	2	3	4	5
The usefulness of the information presented?	1	2	3	4	5
Your level of knowledge related to this topic **BEFORE** using this learning tool and/or test?	1	2	3	4	5
Your level of knowledge related to this topic **AFTER** using this learning tool and/or test?	1	2	3	4	5
The overall quality of this learning tool and/or test?	1	2	3	4	5

Fill in the blanks:

What was most valuable about this learning tool or test?

_____
_____
_____
_____

What information needs to be corrected, inserted, removed, or updated?

_____
_____
_____
_____

What could be done to improve or enhance this learning tool or test?

_____
_____
_____
_____